



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.                                     | FILING DATE | FIRST NAMED INVENTOR      | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|---------------------------|---------------------|------------------|
| 09/879,575  | 06/12/2001  | James Alexander Reeds III | 1999-0275           | 4755             |
| 34700   | 7590        | 08/10/2005                | EXAMINER            |                  |
| DOCKET CLERK<br>P.O. BOX 802432<br>DALLAS, TX 75380 |             |                           | TRAN, ELLEN C       |                  |
|   |             |                           | ART UNIT            | PAPER NUMBER     |
|   |             |                           | 2134                |                  |

DATE MAILED: 08/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/879,575

Applicant(s)

REEDS ET AL.

Examiner

Ellen C. Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 02 May 2005.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-53 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-53 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

***DETAILED ACTION***

1. This action is responsive to communication: 2 May 2005 with acknowledgement of an original application filed 12 June 2001.

2. Claims 1-53 are currently pending in this application. Claims 1, 14, 33, 41, 48, 49, and 53 are independent claims.

***Response to Arguments***

3. Applicant's arguments with respect to claims 33-48 (35 USC § 101 rejection) and respect to claims 4, 17, 25-32, 36, and 44 (35 USC § 112 2<sup>nd</sup> paragraph rejection), have been considered but are not persuasive.

In response to applicant's argument beginning on page 16, "Claims 33-40 are directed to a receiver, which is a specific hardware device (which can utilize software components) ... Claims 41-47 are directed to a transmitter ... Therefore, the non-statutory subject matter rejection is traversed". The Office disagrees the applicant is claiming apparatus such as a receiver or a transmitter utilizing the method of a software program. To overcome this rejection the applicant needs to amend the claims so that the language in the body of the claims links the apparatus to perform an operation. The Examiner notes that in this Office Action the claims rejected under 101 have been increase to include all independent claims.

In response to applicant's argument beginning on page 18, "First, Applicant notes that this appears to be a claim—indefiniteness rejection, as per 112 second paragraph ... Claims 2-4 and their dependents, then further describe ways in which the "applying" process can be performed at least in part. Applicant believes this interrelation between the "applying" process of claim 1 and further limitation in the dependent claims to be clear and definite to those of skill

Art Unit: 2134

in the art". This 112 rejection will be dropped. However the Office notes the use of the words decryption and encryption in claims 1 and 2 respectively raises concerns that steps might be missing from the application or that the terms were used incorrectly because a decryption method by applying an encryption function does not correlate with the literal meaning of the word used. A decryption method is to bring previously encrypted data into plaintext. Claims 1 and 2 as written claim: "A method comprising ... decrypting a payload ... by applying ... wherein the applying further comprises performing an encryption process".

In response to applicant's argument beginning on page 19, "Indeed, even a quick search of USPTO database shows that multiple issued patents include claims that reference RC4, using the term to refer to the well-known cipher and not to a particular material or product". The Office disagrees RC4 is a trademark see cited reference from the Internet, a trademark should not be used in the claims. To overcome this rejection applicant needs to indicate the specific definition of the algorithm relied upon. RC4 is owned by RSA therefore nothing prevents RSA from changing the definition of the term RC4 that is why use of the term in the claims is incorrect.

4. Applicant's arguments with respect to 35 USC § 102 rejection on claims 1-53 have been considered but are moot in view of the new ground(s) of rejection.

#### ***Response to Amendment***

The amendment to the claims filed on 2 May 2005 does not comply with the requirements of 37 CFR 1.121(c) because applicant indicated on the claim sheet "Following are the current claims. For the claims that have NOT been amended in this response, any differences

Art Unit: 2134

in the claims below and the current state of the claims is unintentional and in the nature or a typographical error". In addition on claim 22, the claim indicates (Original) however on line 2 the abbreviation "2D" was added so that the phrase reads "to the encrypted 2D data packet" no support was shown in the specification for a 2D data packet. Therefore the amendment, which was not indicated on the claim sheet will be disregarded. Amendments to the claims filed on or after July 30, 2003 must comply with 37 CFR 1.121(c) which states:

(c) *Claims.* Amendments to a claim must be made by rewriting the entire claim with all changes (e.g., additions and deletions) as indicated in this subsection, except when the claim is being canceled. Each amendment document that includes a change to an existing claim, cancellation of an existing claim or addition of a new claim, must include a complete listing of all claims ever presented, including the text of all pending and withdrawn claims, in the application. The claim listing, including the text of the claims, in the amendment document will serve to replace all prior versions of the claims, in the application. In the claim listing, the status of every claim must be indicated after its claim number by using one of the following identifiers in a parenthetical expression: (Original), (Currently amended), (Canceled), (Withdrawn), (Previously presented), (New), and (Not entered).

(1) *Claim listing.* All of the claims presented in a claim listing shall be presented in ascending numerical order. Consecutive claims having the same status of "canceled" or "not entered" may be aggregated into one statement (e.g., Claims 1–5 (canceled)). The claim listing shall commence on a separate sheet of the amendment document and the sheet(s) that contain the text of any part of the claims shall not contain any other part of the amendment.

(2) *When claim text with markings is required.* All claims being currently amended in an amendment paper shall be presented in the claim listing, indicate a status of "currently amended," and be submitted with markings to indicate the changes that have been made relative to the immediate prior version of the claims. The text of any added subject matter must be shown by underlining the added text. The text of any deleted matter must be shown by strike-through except that double brackets placed before and after the deleted characters may be used to show deletion of five or fewer consecutive characters. The text of any deleted subject matter must be shown by being placed within double brackets if strike-through cannot be easily perceived. Only claims having the status of "currently amended," or "withdrawn" if also being amended, shall include markings. If a withdrawn claim is currently amended, its status in the claim listing may be identified as "withdrawn—currently amended."

(3) *When claim text in clean version is required.* The text of all pending claims not being currently amended shall be presented in the claim listing in clean version, i.e., without any markings in the presentation of text. The presentation of a clean version of any claim having the status of "original," "withdrawn" or "previously presented" will constitute an assertion that it has not been changed relative to the immediate prior version, except to omit markings that may

Art Unit: 2134

have been present in the immediate prior version of the claims of the status of “withdrawn” or “previously presented.” Any claim added by amendment must be indicated with the status of “new” and presented in clean version, *i.e.*, without any underlining.

(4) *When claim text shall not be presented; canceling a claim.*

(i) No claim text shall be presented for any claim in the claim listing with the status of “canceled” or “not entered.”

(ii) Cancellation of a claim shall be effected by an instruction to cancel a particular claim number. Identifying the status of a claim in the claim listing as “canceled” will constitute an instruction to cancel the claim.

(5) *Reinstatement of previously canceled claim.* A claim which was previously canceled may be reinstated only by adding the claim as a “new” claim with a new claim number.

### *Claim Rejections - 35 USC § 101*

5. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 1-53 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Independent claims 1, 14, 33, 41, 48, 49, and 53 are directed to a method comprising: “a session count evaluator configured” and “a decryption engine”. The terminology used as well as the description in the specification indicates that the session count evaluator and the decryption engine are nothing more than a computer program or software. In order to overcome this rejection applicant must show that a component or device is needed to perform the language claimed, in addition applicant needs to show how the device or equipment is needed to perform the steps.

### *Claim Rejections - 35 USC § 112*

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Art Unit: 2134

8. Claims 1-53 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. All the independent claims contain the phrase "fixed length segment" followed by using "a portion of the fixed length segment" there is not any indication how this portion is selected and there is no further description of a fixed length segment.

9. Claims 4, 17, 25-32, 36, and 44 contain the trademark/trade name "RC4" owned by RSA. Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe a proprietary standard for stream cipher and, accordingly, the identification/description is indefinite. As discussed previously RC4 is a trademark it should not be in the claims. The applicant can overcome this rejection by providing a specification of RC4 algorithm.

10. To expedite a complete examination of the instant application the claims rejected under 35 U.S.C. 101 (nonstatutory) as well as 35 U.S.C. 112 above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

***Claim Rejections - 35 USC § 102***

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

12. **Claims 1-8, 14-27, 33-39, 41-51, and 53** are rejected under 35 U.S.C. 102(e) as being anticipated by Medvinsky U.S. Patent Application Publication No. 2002/0094081 (hereinafter '081).

As to independent claim 1, **“A method comprising: selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet”** is taught in '081 pages 3-4 paragraphs 0033-0034;

**“and decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet”** is shown in '081 page 2, paragraphs 0017-0018.

As to dependent claim 2, **“wherein the applying comprises performing a bit per bit streaming encryption process”** is disclosed in '081 page 3, paragraph 0034.

As to dependent claim 3, **“wherein the applying further comprises performing an exclusive OR operation with the portion of the fixed length segment and the data packet”** is taught in '081 page 3, paragraph 0034.

As to dependent claim 4, **“wherein the applying further comprises performing an RC4 operation with the portion of the fixed length segment and the data packet”** is shown in '081 page 3, paragraph 0034.



Art Unit: 2134

As to dependent claim 5, “further comprising: receiving the data packet, the data packet comprising at least a portion of the received session count” is shown in ‘081 page 2, paragraphs 0017-0018.

As to dependent claim 6, “wherein the data packet further comprise at least a portion of a received message digest value” is disclosed in ‘081 page 4, paragraph 0054.

As to dependent claim 7 “wherein the selecting comprises: selecting a current fixed length segment if a difference between the received session count and a locally generated session count is less than a threshold value” is shown in ‘081 page 4, paragraphs 0036-0051.

As to dependent claim 8, “wherein the selecting further comprises: extracting the at least a portion of the received session count from the encrypted data packet; expanding the at least a portion of the received session count to the received session count; and comparing the received session count to the locally generated session count” is disclosed in ‘081 pages 3-4 paragraphs 0033-0034.

As to independent claim 14, “A method of generating an encrypted data packet, the method comprising: selecting a fixed length segment of a continuous encryption key stream” is taught in ‘081 pages 3-4 paragraphs 0033-0034;

“applying a portion of the fixed length segment to data to form an encrypted payload; generating a session count based in accordance with the fixed length segment; and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet” is shown in ‘081 page 2, paragraphs 0017-0018.

As to dependent claims 15, 16, and 17, these claims contain substantially similar subject matter as claims 2, 3, and 4; therefore they are rejected along the same rationale.

Art Unit: 2134

As to dependent claim 18, “further comprising: generating a message digest value; and combining at least a portion of the message digest value with the encrypted payload to form the encrypted data packet” is taught in ‘081 page 4, paragraphs 0054 –0055.

As to dependent claim 19, “wherein the generating comprises: generating the message digest value based on the encrypted payload, the session count and a message digest key” is shown in ‘081 page 4, paragraphs 0054 –0055.

As to dependent claim 20, “further comprising: forming the at least a portion of the message digest value by truncating the message digest value” is disclosed in ‘081 page 4, paragraphs 0054 –0055.

As to dependent claim 21, “further comprising transmitting the encrypted data packet to a receiver through a communication channel” is taught in ‘081 page 2, paragraph 0016.

As to dependent claim 22, “further comprising: receiving a received data packet corresponding to the encrypted data packet, the received data packet comprising the encrypted payload, at least a portion of a received session count and a received truncated message digest value; selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet; and decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet” is shown in ‘081 pages 3-4 paragraphs 0033-0034 and page 4, paragraphs 0053-0055.

As to dependent claims 23-27, these claims contain substantially similar subject matter as claims 2-8; therefore they are rejected along the same rationale.

As to independent claim 33, **“A receiver comprising: a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold”** is taught in ‘081 pages 3-4 paragraphs 0033-0034;

**“and a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold”** is shown in ‘081 page 2, paragraphs 0017-0018.

As to dependent claims 34-39 these claims contain substantially similar subject matter as claims 2-8; therefore they are rejected along the same rationale.

As to independent claim 41, this claim is directed to a transmitter of the method of claim 14; therefore it is rejected along similar rationale.

As to dependent claims 42-51, these claims contain substantially similar subject matter as claims 2-8; therefore they are rejected along the same rationale.

As to independent claim 48, is directed to a system consisting of independent claims 33 and 41; therefore it is rejected along the same rationale.

As to independent claim 49, **“A method comprising: receiving a data packet through a communication channel”** is taught in page 2, paragraph 0016;

**“the data packet comprising at least a portion of a session count; selecting a fixed length segment of a continuous decryption key stream based on the session count”** is taught in ‘081 pages 3-4 paragraphs 0033-0034;

Art Unit: 2134

**“and applying a portion of the fixed length segment by performing a bit per bit streaming encryption to decrypt a payload of the data packet”** is shown in ‘081 page 2, paragraphs 0017-0018.

As to dependent claims 50 and 51, these claims contain substantially similar subject matter as claims 7 and 8; therefore they are rejected along the same rationale.

As to independent claim 53, **“A method of generating an encrypted data packet, the method comprising: selecting a fixed length segment of a continuous encryption key stream”** is taught in ‘081 pages 3-4 paragraphs 0033-0034;

**“applying a portion of the fixed length segment to data by performing a bit per bit streaming encryption process to form an encrypted payload; generating a session count in accordance with the fixed length segment; and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet”** is shown in ‘081 page 2, paragraphs 0017-0018.

### ***Claim Rejections - 35 USC § 103***

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

14. Claims 9-13, 28-32, 40, and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘252 in further view of Chang et al. U.S. Patent 6,105,012 (hereinafter ‘012).

**As to dependent claim 9, “further comprising: discarding the data packet if the difference is not less than the threshold value”** however ‘127 teaches “The key check block is sent to the receiver as a header of the current encrypted data payload. The receiver also retains the last eight bytes of the current packet, it decrypted the first eight bytes (the key check block) and compares the result to the retained last eight bytes ... If there is no match, an error occurred and the receiver takes appropriate action” on page 5, paragraph 0052.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method key selection for decryption taught in ‘081 to include a means to compare the keys being used and take appropriate action (i.e. delete packet) when a match is not found. One of ordinary skill in the art would have been motivated to perform such a modification because of the need to protect data during transmission see ‘127 (page 1, paragraphs 0005-0006). “It is known to remedy this deficiency by decrypting the data field of the packet with the current session key, as well as the next key in the sequence of keys, and choose the key for which the decrypted data makes sense. Using this method, the change-over from one session key to the next is automatically detected. However, to determine whether the decrypted data makes sense requires knowledge about the information being transmitted. This is not always the case, limiting the use of this method. It is an object of the invention to provide a secure communication system, sink device and secure communication method which overcome above mentioned drawback”.

**As to dependent claim 10, “further comprising: re-synchronizing a decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the difference is not less than the threshold value”** is taught in ‘081 page 4,

Art Unit: 2134

paragraphs 0041- 0053 “it signals the CODEC change to gateway controller 106. MTA 104 generates a new set of RTP key stream and a new initial time stamp. Herein lies a first advantage of the present invention. The related art provides for re-derivation of the RTP key stream when a CODEC change occurs, by providing the following key derivation function ... “End-End RTP Key Change <N>” is a label that is used as a parameter to the key derivation function”.

**As to dependent claim 11, “further comprising: discarding the data packet if the at least a portion of the received message digest value does not match a locally generated message digest value”** is taught in ‘127 page 5, paragraph 0052-0053.

**As to dependent claim 12, “further comprising: re-synchronizing the decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the at least a portion of the received message digest value does not match the locally generated message digest value”** is shown in ‘081 page 4, paragraph 4-5, paragraphs 0054-0057 “In a further embodiment, the above solution is employed for a MAC (Message Authentication Code) algorithm change, resulting in a packet size change. Traditionally, for convenience the same RC4 key stream may be used in the generation of the keying material needed to calculate a MAC for each packet (a MAC is appended after the encrypted text). Where the MAC pad is key used to generate the MAC, for one-time use only. So, wehre a key stream is used for MAC generation (instead of or in addition to encryption) and the size of that random pad changes, one must rekey and start a new RC4 key stream in the same way as fro CODE changes”.

As to dependent claim 13, “further comprising: extracting the at least a portion of the received message digest value from the data packet; generating the locally generated message digest value based on the at least a portion of the received session count, a received encrypted payload of the data packet and a message digest key; truncating the locally generated message digest value to form a truncated message digest; and comparing the truncated message digest to the at least a portion of the received message digest value” is shown in ‘081 page 4, paragraph 4-5, paragraphs 0054-0057.

As to dependent claims 28-32, these claims contain substantially similar subject matter as claims 9-13; therefore they are rejected along the same rationale.

As to dependent claim 40, “further comprising: a message digest extractor configured to extract the at least a portion of the received message digest value from the received encrypted data packet” is taught in ‘081 page 4, paragraph 0054 “In a further embodiment, the above solution is employed for a MAC (message Authentication Code) algorithm change, resulting a in a packet size change”;

“a message digest generator configured to generate a locally generated message digest value based on the at least a portion of the session count, a received encrypted payload of the data packet and a message digest key” is shown in ‘081 pages 4-5 paragraph 0055-0056 “For example, additional key stream bytes may be allocated to calculate a MAC for each frame. However, ehre is only one MAC needed for the whole RTP packet and if an RTP packet contains multiple frames only the key stream bytes allocated to one of the frames ...

Where the MAC pad is a key used to generate the MAC, for one-time use only;

**“a truncator configured to truncate the locally generated message digest value to form a truncated message digest; and a message digest evaluator configured to compare the truncated message digest value to the at least a portion of the received message digest value”** is disclosed in ‘081 page 5, paragraph 0057 “one must rekey and start a new RC4 key stream in the same way as fro CODEC changes”;

**“where the received is configured to discard the received encrypted data packed it the truncated message digest value does not match the at least a portion of the received message digest value”** is taught in ‘127 page 5, paragraph 0052 “The key check block is sent to the receiver as a header of the current encrypted data payload. The receiver also retains the last eight bytes of the current packet, it decrypted the first eight bytes (the key check block) and compares the result to the retained last eight bytes ... If there is no match, an error occurred and the receiver takes appropriate action”.

As to dependent claim 52, **“further comprising discarding the data packet if the difference is not less than the threshold value”** is taught in ‘127 page 5 paragraph 0052.

### *Conclusion*

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 1:30 pm.

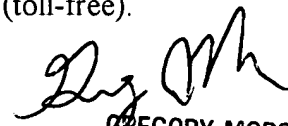
If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.



Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran  
Patent Examiner  
Technology Center 2134  
23 July 2005

  
GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2134